REMARKS

By this Amendment, claims 1, 28, 55, and 82 are being amended to further define the claimed subject matter. Claims 1, 4, 6-28, 31, 33-55, 58, 60-82, and 87-107 are pending in this application.

Applicants respectfully traverse the rejection of claims 1, 4, 6-28, 31, 33-55, 58, 60-82, 85, and 87-107 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,542,610 to Traw et al. ("*Traw et al.*") in view of U.S. Patent No. 5,412,730 to Jones ("*Jones*").

Traw et al. fails to teach or suggest each and every element recited in independent claim 1 as amended, from which claims 4 and 6-27 depend. For example, *Traw et al.* fails to teach or suggest an information processing system wherein, inter alia, "the encrypted data is encrypted using an encryption key, the encryption key being formed based on a first random number generated by the first information processing apparatus and a second random number generated by the second information processing apparatus, the second random number being different from the first random number, and then the encrypted data is transmitted in the isochronous transmission mode via the interface," as recited in amended claim 1 (emphasis added).

Instead, *Traw et al.* teaches a "method for protecting digital content from copying and/or other misuse as it is transferred between one or more computationally constrained deices over insecure links" (Abstract). The method includes establishing an encrypted control channel to preserve confidentiality of content channel keys (Col. 9, lines 53-59.) The "source of the content" sends a content channel key that is "a randomly generated key which is unique for each stream of content ($K_{Content}$)" (Col. 9, lines 59-64).

The Examiner acknowledges, "Traw does not explicitly disclose the encryption key used for decrypting the content is generated by a second random number generated by the second information apparatus" (Office Action of May 31, 2006, pg. 4, paragraph 2), relying on *Jones* to make up for these deficiencies.

However, *Jones* does not make up for the deficiencies of *Traw et al.* because *Jones* also fails to teach or suggest, "the encrypted data is encrypted using an encryption key, the encryption key being formed based on a first random number generated by the first information processing apparatus and a second random number generated by the second information processing apparatus, the second random number being different from the first random number, and then the encrypted data is transmitted in the isochronous transmission mode via the interface," as recited in claim 1 (emphasis added).

Instead, *Jones* teaches a data transmission system in which "keys may be generated by a random number generator located at the transmitting end, encrypted in accordance with the currently active key, and transmitted along with the other data. At the receiving station, the encrypted key is extracted from the data stream, deciphered, and substituted at a designated time for the prior key." (Col. 1, lines 12-14 and lines 22-33.) "[P]seudo-random number generators [23, 27] are employed at both the transmitting and receiving stations [11, 12] to supply a like sequence of encryption keys to both the encryptor [17] and decryptor [31]" (col. 1, lines 37-41). "[T]o permit the two stations to communicate, each supplied [sic] in advance with a random number seed value which exclusively determines the numerical content of the sequence of numeric values generated by each of the two pseudo-random generators" (col. 1, lines 43-48).

"[T]he two generators switch from one output key value to the next in synchronism" (col. 1, lines 48-49; emphasis added).

The encryption key supplied to the encryptor at the transmitting station of *Jones* is not "formed based on a first random number generated by the first information processing apparatus and a second random number generated by the second information processing apparatus, the second random number being different from the first random number," as required by claim 1. Rather, the encryptor (17) of *Jones* receives only a single sequence of encryption keys from the pseudo-random generator (23) at the transmitting station. Furthermore, the pseudo-random number generator (27) of *Jones* consistently supplies the same encryption key as the pseudo-random number generator (23). An encryption key that is a single pseudo-random number generated by a single pseudo-random number generator does not constitute an encryption key "formed based on a first random number generated by the first information processing apparatus and a second random number generated by the second information processing apparatus, the second random number being different from the first random number," as required by claim 1 (emphasis added).

Thus, since *Traw et al.* and *Jones* fail to teach or suggest, alone or in combination, "the encrypted data is encrypted using an encryption key, the encryption key being formed based on a first random number generated by the first information processing apparatus and a second random number generated by the second information processing apparatus, the second random number being different from the first random number, and then the encrypted data is transmitted in the isochronous

transmission mode via the interface," as recited in claim 1, claim 1 and claims 4 and 6-27 that depend therefrom are allowable over *Traw et al.* and *Jones*.

Claims 28, 55, and 82 should be allowed over *Traw et al.* and *Jones* under § 103(a) for reasons substantially similar to those explained above. *Traw et al.* and *Jones* fail to teach or suggest, alone or in combination, the "encryption key being formed based on a first random number generated by the first information processing apparatus and a second random number generated by the second information processing apparatus, the second random number being different from the first random number," recited in claims 28, 55, and 82 (emphasis added). Thus, claims 28, 55, and 82, and claims 31, 33-54, 58, 60-81, 85, and 87-107 that depend therefrom, should also be allowed over *Traw et al.* and *Jones*.

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Dated: October 2, 2006

By: _____

Reece Nienstadt
Reg. No. 52,072